THE NEW ATLANTIS
A JOURNAL OF TECHNOLOGY & SOCIETY

Liberty, Privacy, and DNA Databases

Christine Rosen

Imagine the following scenario: You happen to match the physical description of a serial burglar who has been preying recently upon residents of a suburb of Richmond, Virginia. After being brought in for questioning by the police, you are asked to participate in a line-up, whereupon an eyewitness identifies you as the culprit. The police place you under arrest. The next day, the real burglar is apprehended, and you are freed—a simple case of mistaken identity. But you will have left something behind: your DNA, which the police have taken from you at arrest and stored in the state's criminal database in the form of a DNA "fingerprint."

Or consider this: Like thousands of other Americans, you voluntarily donate a DNA sample to a large medical research study, assured by the directors of the study that your information will remain anonymous, your genetic privacy secured in an unbreakable DNA database accessed only by approved researchers. A few months later you are placed under arrest for attempted murder; one of your former sexual partners has tested positive for HIV, and you are charged with knowingly infecting her with the virus. The evidence for this charge? The supposedly anonymous DNA sample you gave to the medical researchers, which the police tracked down and tested for evidence of HIV.

Or perhaps you are like the woman whose mother and aunt both suffered from breast cancer. Wanting to know her genetic risk for the disease, she sent in a blood sample to a private lab to be DNA-tested for the mutant genes—BRCA1, BRCA2, and BRCA3—that have been found to increase a woman's risk of breast cancer by as much as sixteen times. The company that performed the test assured her that her sample would remain anonymous, the results known only to her, although the disclaimer she signed offered few specifics about these privacy protections. Four years later, she is denied insurance coverage. Why? The insurance company purchased the private lab's DNA database, ostensibly for research purposes, and cross-referenced it with its own. They red-flagged the names of people who had been tested for breast cancer.

Such scenarios carry the whiff of mediocre Hollywood screenplays, but they are closer to truth than fiction. Beginning in 2003, anyone arrested for a felony in the state of Virginia must relinquish a DNA sample for the state's forensic database. The second scenario actually happened in Scotland, where a prisoner who had voluntarily offered a DNA sample for research, on the condition that his identity remain anonymous, was later prosecuted for knowingly infecting a

---

Christine Rosen *is a senior editor of* The New Atlantis *and resident fellow at the Ethics and Public Policy Center.*

woman with HIV; the evidence used to prosecute him came from the supposedly anonymous sample he contributed to the research study, which prosecutors decoded and introduced in the trial. The final example is hypothetical, but the architecture is already in place for it to become a reality.

Fifty years have passed since Watson and Crick discovered the structure of DNA, and the double helix has replaced the caduceus as the symbol of scientific and medical progress. We have mapped the human genome and embarked on identifying and curing heretofore intractable genetic conditions. With startling swiftness we have also constructed DNA databases and storage banks to manage the genetic information generated by these discoveries. The most zealous advocates for these new technologies imagine only the endless possibilities: We will solve and deter crime; we will rescue the falsely convicted from prison sentences or execution; we will uncover our genetic ancestry; we will map, understand, and cure dreaded diseases; we will tailor pharmaceuticals according to each individual's genetic make-up; we will gain crucial understanding about the respective role of nature and nurture in shaping human identity; and we will create the "genetic economy of the future."

So far, the public discussion of DNA fingerprinting has focused largely on its uses within the criminal justice system. In the U.S., the first criminal conviction based on DNA evidence came in 1987. The battles in the late 1980s and early 1990s over the effectiveness and accuracy of DNA as forensic evidence—infamously featured in the televised murder trial of O. J. Simpson—proved in the end to be merely a splendid little war. Courts quickly embraced DNA evidence as legally admissible, and legislatures were soon responding to law enforcement's claims that they needed DNA databases to manage this new and powerful form of forensic information. Within ten years of that first conviction, all fifty states required convicted felons to submit DNA samples; soon every state had established its own criminal DNA database.

In 1994, the DNA Identification Act established a national DNA database, run by the FBI, called CODIS (Combined DNA Identification System), which links all state databases. Today, the newspapers regularly bring stories of a murderer identified through a "cold hit" on a DNA database, or an innocent man freed from prison after DNA evidence exonerates him. In March 2003, Attorney General John Ashcroft announced a new initiative, "Advancing Justice Through DNA Technology," that seeks $1 billion over the next five years to aid in "realizing the full potential of DNA technology to solve crime and protect innocent people." Media coverage focused on the initiative's efforts to eliminate the backlog of DNA samples at state and federal criminal laboratories, but the initiative seeks something else as well: the expansion of CODIS. The Bush administration is keen on giving the FBI access to the full range of samples in state DNA databases—including those of people placed under arrest but not convicted—rather than the smaller range of samples currently included.

But in focusing so much on dramatic stories of finding the guilty and freeing the innocent—or the prospect of using genetic information to cure disease—we risk obscuring the full significance and inherent dangers of DNA technology. While the creation of DNA databases often can be defended case-by-case, the development of this technology serves an end in itself apart from any particular application. It provides an inescapable means of identification, categorization, and profiling, and it does so with a type of information that is revelatory in a way few things are. As bioethicist George Annas put it, DNA is a person's "future diary." It provides genetic information unique to each person; it has the potential to reveal to third parties a person's predisposition to illnesses or behaviors without the person's knowledge; and it is permanent information, deeply personal, with predictive powers. Taken together, the coming age of DNA technology will change the character of human life, both for better and for worse, in ways that we are only beginning to imagine—both because of what it will tell us for certain and what it will make us believe. To know one's own future diary—or to know someone else's—is to call into question the very meaning and possibility of human liberty.

Crime, Punishment, and DNA

A British scientist, Alec Jeffreys, first perfected the technique of using DNA samples to extract a unique marker—sometimes called a "genetic fingerprint"—that ensured nearly absolute proof of identification. After the brutal rape and murder of two young women in the small English village of Narborough in 1986, police used Jeffreys's DNA fingerprinting method to locate the culprit. In their search for the killer, they performed the world's first genetic dragnet, "blooding" more than 4,000 men in Narborough and its environs until they found the person who matched the genetic profile of the killer. The U.K. went on to create a national criminal DNA database in 1995. It currently houses more than 1.5 million DNA profiles of convicted felons; by 2004 it should have three million.

In the U.S., all fifty states currently have criminal DNA databases, although each state has different requirements for collecting samples. Some states collect samples only from those convicted of sex offenses or violent crimes; others require sampling of all convicted felons; a few states even take samples from juveniles convicted of crimes that would be considered felonies had they committed them as adults.

If DNA databases are the most revolutionary force in crime fighting in a generation, Dr. Paul Ferrara is arguably that revolution's leader. (He had just gotten off the phone with best-selling crime novelist Patricia Cornwell when I spoke to him. "She was double-checking a few forensics things for her Jack the Ripper book.") As head of Virginia's Division of Forensic Science, he oversees the largest and oldest state DNA criminal database in the country—although

old, in this context, means adolescent. The database has been up and running since 1989, one year after Virginia sentenced to death Timothy Spencer, the "South Side Strangler," based on DNA evidence found at a murder scene.

The first Virginia database stored DNA samples only from convicted sex offenders, but within a year, the law had expanded to require DNA samples from all adult felons. Juveniles over the age of fourteen who committed serious crimes were added in 1996, and beginning in January 2003, any person *arrested* for a violent felony or burglary must give the state their DNA. When I asked Ferrara whether he was concerned about the compulsory sampling of people who were, by law, innocent until proven guilty, he replied that "these expansions were all passed by the legislature." Besides, he noted, "the sample and records of those arrested are destroyed if the charges are dismissed."

This is small reassurance for civil liberties activists. Testifying before Congress about the expansion of CODIS, director of the American Civil Liberties Union's Technology and Liberty Program Barry Steinhardt argued, "While DNA databases may be useful to identify criminals, I am skeptical that we will ward off the temptation to expand their use." "We have already entered the realm of the Brave New World," he said, urging Congress to "turn back" from expanding these databases further. Such critics argue that mandatory DNA sampling of suspects and felons fundamentally changes the way government treats its citizens. "The state is saying, in effect, you may be a danger in the future because you were in the past, and therefore we need to register your DNA," Boston public defender Benjamin Keehn argued on PBS NewsHour. "If we are going to take DNA from prisoners because they are at-risk [of committing crimes in the future], why shouldn't we take DNA from teenagers, from homeless people, from Catholic priests, from any subgroup of society that someone is able to make a statistical argument of being at-risk?"

Ferrara is not overly exercised by these civil liberties concerns. "The ACLU is concerned this is a slippery slope," he said. "Well, they're right. That's probably the pattern that will continue. But is that slippery slope a bad thing? I don't think so." Ferrara believes such debates are better left to politicians—politicians who are easily persuaded by the evidence he gives them. "Look, it's a policy question," he said. "I'm a technocrat, and it's true that the data we generate—the cold hit rate, the number of crimes solved—do impact the opinion of the legislators. But policymakers are going to have to make these decisions." His primary concern is eliminating the backlog of DNA samples required to expand and digitize the state's database.

At least three big questions, however, have not been adequately addressed. First, the evidence of DNA's effectiveness as a crime-fighting tool is at once impressive and ambiguous, depending on how the genetic information is used.

DNA evidence, when used to incriminate or exonerate suspects already identified by more traditional police work, is extraordinarily useful. "Our forensic scientists can identify an individual from objects such as a half-eaten chicken sandwich, urine in the snow … or even cross-transfer of DNA from a handshake," Ferrara recently boasted to Congress. But the verdict is less clear when it comes to *DNA databases*, which attempt to match DNA evidence found at the crime scene with preexisting DNA records. *USA Today* recently reviewed the criminal DNA database system and found wide variations in effectiveness from state to state. Even worse, officials do not in fact know how many of the "cold hits"—the unexpected matches made when a law enforcement official plugs evidence from old, unsolved cases into a database—end in actual convictions. No one is tracking what happens once a DNA database match is made. "We try to track cold hits to conviction," Paul Ferrara says, "but we really have not had the opportunity or resources to really study and follow statistically the actual impact." In effect, state legislatures, impressed by stories of "cold hits," are being persuaded to expand these databases with no real statistical evidence as to their effectiveness in ultimately convicting criminals.

Second, the claims by proponents of DNA databases that the genetic information used for DNA fingerprints is merely "junk DNA"—hence not capable of revealing an individual's genetic predispositions—is not the whole truth. Buried in a genetics journal from a few years ago is a report by a team of British scientists that "the standard DNA fingerprints used by police around the world contain a subtle signature which can be linked to a person's susceptibility to Type 1 diabetes." Alec Jeffreys, the progenitor of junk DNA fingerprinting, was part of the research team that made the discovery. Jeffreys predicted that "further troubling links between DNA fingerprints and disease will emerge as scientists probe the completed draft of the human genome." One person's "junk" DNA might prove to be another's future wealth of information about genetic conditions.

Finally, we must reckon with the craftiness and adaptability of the criminal mind, which already is trying to outsmart forensic DNA technologies. As *USA Today* recently reported, law enforcement officers in Richmond have found prisoners taking DNA tests for other prisoners, while jailers in Utah have listened in on conversations among prisoners about how to fool the police by planting someone else's blood or semen at the scene of a crime. The most notorious episode to date occurred in Milwaukee, where an inmate intent on undermining the DNA evidence used in his rape conviction had a relative smuggle his semen out of jail in a ketchup packet, then stage a false rape using the sample so that the inmate could argue that he was being set up. After all, how could a man in prison leave DNA evidence at the scene of a crime committed miles away unless he was being framed?

Law enforcement generally characterizes the debate over DNA databases as

a choice about how "tough on crime" we wish to be. Discussing proposed legislation to expand the state of Utah's DNA database to include all felons—including those incarcerated, on parole, and on probation—the state representative who helped craft the bill declared: "We're going to protect people. We're going to stop people from getting raped. We're going to stop people from being victimized." Last year, a sheriff in Salt Lake County, Utah, told the local paper, "I would like to take a DNA sample from everyone that gets booked into my jail." Most law enforcement professionals would like to see these DNA databases integrated and linked to databases of criminal history, license plate records, and myriad other public records.

The legal fights about the uses of DNA, both criminal and civilian, are most likely just beginning. In November 2002, for example, a federal judge in Sacramento, California, ruled in favor of Danny Miles, a convicted felon sentenced to probation who refused to provide a DNA sample to his probation officer. The sample was required by the DNA Analysis Backlog Elimination Act, which President Clinton signed into law in 2000. U.S. District Judge William Shubb found persuasive Miles's claim that compulsory DNA sampling violated his Fourth Amendment protections against unreasonable search and seizure.

In addition, the courts have not yet ruled on a far greater problem: the lack of consistent privacy protections for criminal databases and their samples. Currently, the states have a patchwork of protections for their databases, but only a few have thorough regulations for monitoring the privacy of the original samples drawn from the convicted. "Forensic DNA databanks are more highly regulated and protected than any other kind of databanks," Paul Ferrara assured me. "The greater threat to privacy is the ability of unscrupulous people to retrieve others' DNA surreptitiously," as happened recently in a tabloid-style paternity case involving Hollywood producer Steve Bing; a private investigator pilfered his discarded dental floss from the garbage for DNA paternity testing.

But there are serious problems with even these regulated databanks and databases: few have adequate privacy protections; there is no national oversight of the quality of samples or the databases themselves; and there are no consistent regulations regarding who can access information and for what reasons. Implementing three simple practices (all endorsed by the ACLU) would go a long way toward preventing misuse of forensic DNA databases: destruction of the original samples taken; restricting the information stored in the CODIS database to convicted violent felons only; and guarantees that the database would be available to individuals, especially those who did not have access to DNA testing when they were convicted, for purposes of exoneration. But so far, there seems to be no overwhelming public demand for such reforms; most people see DNA fingerprinting as the ultimate crime-fighting tool rather than a potential threat to their liberties. And while there is surely a difference between

collecting information on large social groups deemed to be "high-risk" and collecting information on individual criminals and suspects, the rapid expansion of these DNA databases should at least give us pause.

The Universal Database

Besides criminals, two other populations are subject to compulsory DNA sampling: military recruits and newborns. All military personnel are required to submit genetic samples to the Department of Defense for entry into the Pentagon's DNA database. The creation of the database was prompted in part by the challenge the military faced in identifying remains during the first Gulf War, and its avowed purpose is to expedite identification of remains in future conflicts. Tomorrow's wars will have no unknown soldiers, and some unknown soldiers killed in past conflicts are being identified. On May 14, 1998, the Tomb of the Unknowns at Arlington National Cemetery was opened and the twenty-six-year-old remains of Air Force 1st Lt. Michael J. Blassie were exhumed and identified through DNA testing. The military takes samples from active and reserve duty soldiers, and to date only one feeble protest against the database has occurred: the two soldiers who challenged the requirement to give DNA samples as an unreasonable search and seizure lost their case.

In addition, hospitals routinely draw blood from newborns to test for a range of genetic conditions, and all states have laws that require hospitals to screen for phenylketonuria, an inherited metabolic condition that is easily treatable if found early but causes severe mental retardation and organ damage if it is not. Since the mid-1960s, hospitals have also taken a few drops of blood from infants at birth and preserved them on pieces of paper called "Guthrie cards," which are then tested for genetic conditions such as sickle cell anemia, cystic fibrosis, and muscular dystrophy. But the ultimate fate and potential uses of these samples are uncertain. In June 2002, for example, the state of South Carolina came under fire from privacy advocates when it was revealed that it had collected and was storing indefinitely more than 300,000 such blood samples taken from infants throughout the state.

Taken together, there are many arguments and incentives for expanding these databases at the national level: to aid medical research, to create the biotechnology economy of the future, or to ensure that every falsely accused citizen has a genetic alibi. The U.K. has already embarked on "Biobank," a voluntary national DNA database. The British Government, in conjunction with the Medical Research Council and the Wellcome Trust, is billing Biobank—a database of half a million Britons that will be used to study the interaction of genes, environment, and health—as a boon to medical researchers. Although participation is voluntary, it is not entirely anonymous. "The samples cannot be made strictly anonymous because in order to study the interactions between genes,

environment, and health, the study organizers would have to be able to add information on participants' health to the individual records at a later date," say representatives from the Wellcome Trust. "It is critically important to know which individuals stay healthy and which develop (or die of) particular diseases." In addition, the database will be made available to pharmaceutical and biotechnology companies "to develop new drugs and treatments." GeneWatch UK, a civil liberties watchdog group that focuses on genetics issues, is concerned enough about Biobank that it published an extensive guide of recommended questions that volunteers should ask before submitting samples.

In addition, several countries have sold the rights to their populations' genes to private companies: Iceland famously hawked its citizens' DNA to deCODE Genetics in 2000, and Estonia launched a similar project in 2001, creating a database of nearly all of the country's 1.4 million citizens. Even the citizens of tiny Tonga have sold the rights to their gene pool to an Australian company, Autogen. Some scientists believe these isolated populations offer rich research ground for studying heritable traits, but one cannot help but find disconcerting the nature of such transactions. Their champions do not inspire confidence. DeCODE Genetics founder Kari Stefansson could charitably be described as cavalier about the privacy concerns raised by the creation of these databases. "We have never claimed that the protection of privacy cannot be broken," he told the *New Scientist*. "The principal element here is trust." Thanks in part to an international outcry over the sale of Iceland's genes, and at the urging of Iceland's parliament, Stefansson's company implemented certain privacy protections—and the parliament made identifying individuals on the database a criminal offense, punishable by two years in prison.

But the impulse to bank the DNA of entire nations remains strong. Last fall, Alec Jeffreys criticized the British government for its handling of the country's national DNA database—specifically, for its practice of storing genetic profiles of crime suspects who have been cleared of any wrongdoing. But Jeffreys's proposed solution was not the elimination or downsizing of the DNA database; instead, he called for the creation of a broader national database, managed by an independent body of experts, which would store genetic profiles of the entire British population. "If we're all on the database, we're all in exactly the same boat—the issue of discrimination disappears," he told the BBC. Testifying recently in Washington, D.C., before the President's Council on Bioethics, Baroness Helena Kennedy, Chair of Britain's Human Genetics Commission, remarked on the sanguine approach Britons take to the idea of a universal database. "We are a rather passive, gentle nation it seems," she said, "because nobody has become particularly alarmed enough to make enough of an issue of this." Writing recently in *Nature*, two Australian researchers made a plea for mandatory DNA testing at birth. It would "not only act as a deterrent from crime for

all members of the community," they reasoned, "but would make the task of catching criminals easier for police. If the correct safeguards are in place to protect civil liberties, why should a proposal to test everyone at birth be a frightening one?" James Watson, co-discoverer of the structure of DNA, recently told the *Independent* (U.K.) that he supports the creation of a compulsory international database. "With the increase in terrorism," Watson said, "we want to know who people are."

Despite a stronger tradition of civil liberties and generally greater suspicion of government, the idea of a national DNA database is also gaining support in the United States. Yale University law professor Akhil Amar has argued for the merits of a compulsory national DNA database linked to birth certificate and driver's license records. To allay concerns about abuses, he encourages the creation of a special DNA Court to monitor use. The database would "increase the odds of finding the guilty, freeing the innocent and vindicating the victim," Amar concludes, entirely glossing over the question of protecting original samples and the possibility of "junk DNA" revealing more than simply identity. Others are similarly optimistic about the state's ability to use properly and effectively this powerful new tool. "Instead of thinking of a national database as baring citizens to Big Brother," says Philip Kitcher, in his book, *The Lives to Come*, "we might better view it as the cooperation of the innocent to distinguish, and so protect, themselves from those who perpetrate violent crimes … A national database would also best accord with the demands of justice, refusing to allow some people to be more vulnerable to the law than others." Writing in the *Vermont Law Review*, Jennifer Sue Deck concluded, "It is both feasible and conceivable that the United States Supreme Court would allow the creation of a national DNA databank."

Surely, there is a long way to go from academic speculation to political reality. And it is still possible that Jefferson's heirs will resist the full-scale centralization of our genetic information, even as we desire (or come to expect) the promised benefits of DNA technology. Nevertheless, the momentum for expanding DNA databases is undeniable, while national debate on what this technology means and where it might lead has so far been limited.

Capitalists, Doctors, and Mormons

State initiatives are not the only force driving the expansion of DNA databases. Every day Americans voluntarily submit their genetic material to private groups—medical research institutes, businesses hawking identity genomics services, and religious organizations—for genetic testing, databanking, and database storage. DNA is the raw material for an entire new industry—called "bioinformatics"—initiated by the twin revolutions in genetic mapping and information technology. As early as 1988, the now-defunct Congressional Office of Technology Assessment warned that the IT/genomics sector had spawned ava-

lanches of genetic data that are "persistent and widely shared, and difficult for the subject to know about, to access, to verify, or to correct." Some of these private efforts, especially those dedicated to medical or genealogical research, have privacy protections in place—including guarantees of anonymity and promises never to sell the information to insurance companies or employers. And yet, a wild west of for-profit firms raises serious questions about our capacity to govern the uses of DNA information.

In 2000, DNA Sciences, Inc., a California company with James Watson as one of its founders, launched a website—DNA.com—soliciting volunteer donations to a "Gene Trust." The trust hopes to gather enough samples to study the genetic causes of conditions such as breast cancer, colon cancer, and diabetes. After a volunteer fills out an online questionnaire, DNA Sciences sends a representative to the donor's house to draw a DNA sample, which is then added to the database. The initial response to the company's plea was so overwhelming (over 10,000 people applied) that the Gene Trust is no longer accepting new registrants, instead placing interested parties on a waiting list. Judging by the testimonials on the website, people give samples largely for altruistic reasons. One woman, suffering from breast cancer, hopes that the Gene Trust research will lead to a cure. "What's a little blood?" she mused.

A wide range of DNA databases and DNA banks exist for medical research, much of it directed at curing cancer and heart disease. In 2002, the Mayo Clinic formed a partnership with IBM to develop a genetic database of patient information from the clinic's extensive archival data. Some of these databases, with their capacity to run large-scale epidemiological studies quickly, yield important findings. In August 2002, for example, researchers at the University of California, San Francisco, followed a hunch about hypercholesterolemia—a condition that causes dangerously high cholesterol levels—by searching a 12,000-person genetic database of patients maintained by the UCSF Cardiovascular Research Institute. Using the database, they eventually succeeded in locating the genetic defect that causes the disorder. Longstanding epidemiological studies are also adding genetic database capabilities. The Framingham (Mass.) Heart Study has collected more than 4,000 DNA samples from study participants, and the Nurses' Health Study in Boston has logged more than 100,000 individuals in its database.

The most successful private, voluntary databank so far is the one run by the Church of Jesus Christ of Latter-day Saints. The Mormons collect DNA for their own genealogical purposes, as well as for potential resale to commercial outlets. Once the database is completed, they plan to make the information available to researchers and the public. "We intend for the database to be used broadly for genealogical research," says Dr. Scott Woodward, Professor of Micro and Molecular Biology at Brigham Young University and major organizer of the Molecular Genealogy Research Project (MGRP), which is now wholly funded by

the Sorenson Molecular Genealogy Foundation. "It will assist people in answering difficult genealogical questions." Genealogy is not merely a hobby for Mormons; church teachings encourage believers to seek out ancestors for baptism by proxy.

Woodward admits that potential volunteers occasionally raise privacy concerns. "We try to reassure them about the confidentiality of their samples," he said. "There really isn't an easy way to pull an individual's record out." It is possible, however, and for those staunch skeptics, Woodward says, "our standard answer is—don't participate. You don't have to be part of this." Volunteers in the MGRP have fewer causes for concern than most voluntary DNA donors; the project has an impressive privacy policy. Like most DNA databases, the MGRP replaces all personal names with numbered codes; unlike other databanks and databases, however, the MGRP takes special care to protect the safety of the original DNA samples, which they store in triple-locked freezers. Their database is not linked to the Internet, thus avoiding the potential intrusion of computer hackers. The MGRP's consent form is a model of the species, quick to note possible dangers, such as the fact that the confidentiality of the database might be compromised, as well as leaving open unanticipated future uses (some of them likely lucrative). The database might be used for "medical or health care purposes," the form warns. The MGRP also offers participants the option of refusing to have their samples accessed for non-genealogical research. "Less than five percent of people opt out of that clause," Dr. Woodward told me, with a hint of satisfaction in his voice.

If the Mormon Molecular Genealogy Research Project is a model of a DNA database and bank, its sister for-profit projects in the rough-and-tumble world of free market identity genomics are less so. They are the most unregulated DNA databases and storage banks in the country. The market for identity genomics is growing rapidly, and an ever-proliferating number of private companies now operate extensive DNA databases and DNA banking services. Dale R. Pfost, President and CEO of Orchid Biosciences, a company that offers a wide range of such services, recently told the *Wall Street Transcript* that "identity genomics is the largest existing market for DNA analysis today."

The companies involved range from small, quirky start-ups to multinational behemoths. DNA Analysis, Inc., a company founded in 1989 and based in Ohio, collects genetic samples from the deceased by working with funeral home managers. For $350, they will extract a DNA sample from a deceased person during the embalming process and provide a genetic profile and genetic banking services to the survivors. "Your loved one's DNA is securely stored, at -80 degrees Celsius for a period of 25 years," the company assures. "We were kind of laughed at, at the beginning," admits Bernard G. Naegele, the company's president. "But each year we find more people beginning to understand the value of our service."

The company's website features a picture of a happy family enjoying an afternoon stroll, junior perched charmingly on dad's shoulders, with the slogan, "Helping Families Provide a Lasting Legacy with Advanced Technology." Scrolling down, one finds a picture of a beaming infant and a promise that "the DNA profile you save today may help prevent or even cure the diseases of your children, your grandchildren, and their children." The site carries the endorsement of the Ohio Funeral Directors Association, a slightly macabre Good Housekeeping seal of approval. Nevertheless, Naegele is hopeful that the appeal of DNA banking will continue to expand. "We would like to see DNA banking for every baby born," he said, and spoke enthusiastically of a community in Connecticut that had decided to bank, for posthumous identification purposes, the DNA of its entire Fire Department. Still, he is wary of going too far. "I would not like to see the government say it should be mandatory."

DNA Analysis, Inc., is unique only in its emphasis on the necrotic. A broad range of testing and banking services flourish on the Internet, with names like Genelex, Identagene, and the obvious, if inelegant, Fidelity Test. One company, DNA Lifeprint, offers a DNA "management kit" that allows families to preserve their genetic samples "for generations." The company, founded by a former police officer in Florida, advises parents to have their children's DNA profiles on hand in case of abduction. "Find ways to protect your child from the unthinkable," the website urges. John Walsh, host of the television show "America's Most Wanted," endorses the product. Another organization, Affiliated Genetics, encourages Americans to set up their own, at-home DNA banks. For a mere $19.95 you can purchase a DNA banking kit that allows you to store your sample and those of family members indefinitely at room temperature for the purposes of "future genetic testing."

Companies such as FamilyTree DNA, GeneTree, and Oxford Ancestors offer testing and linkage services for those seeking long-lost ancestors. GeneTree is one of the most successful identity genomics companies in business. Initially started as a genetic counseling and testing service in San Jose, California, GeneTree soon found more lucrative ventures in paternity testing. "We just evolved around the market," says Terry Carmichael, GeneTree's Vice President of Sales and Marketing. "The market wanted biological testing services, so we began offering them." GeneTree started providing at-home DNA testing kits in 1997, and clients wanting paternity testing soon became the company's major customer base. As to the question of whether GeneTree's customers are concerned about their DNA samples falling into the wrong hands, Carmichael says: "Yes and no. Our paternity customers are focused on getting an answer to their question; they don't know or care how the testing is done. They just want a yes or no answer."

As I found when I ordered my own testing package, GeneTree does not exactly encourage its customers to question the ultimate fate of their sensitive

genetic information. My "GeneTree DNA specimen collection kit" arrived in a nondescript, legal-sized manila envelope. Inside, shrink-wrapped in plastic, was an explanatory brochure in a relaxing violet hue and a collection kit, which contained six specimen-collecting "utensils": oversized Q-tips on pastel-colored sticks, color-coded to the enclosed, matching envelopes. The brochure helpfully suggested that "you may want to use the blue envelope and swabs for the alleged father, pink for the mother, and yellow or white for the child."

GeneTree's website includes "an enlightening report on DNA testing using real-life examples from GeneTree customers," with confessional titles such as "Devastated Father Gets His Day in Court," "Bitter Spouse Refuted by the Evidence," and "Entrapment Avoided." As one happy GeneTree customer matter-of-factly related, "I recently found out that my wife had been with another man a few times early in our marriage … our son had been conceived around that time and I kept wondering if he was not my biological son." His torment ended with the sure stroke of the GeneTree swab. "You can't imagine the relief I felt when I read the report that I am indeed his father," he gushed. "We could not be a happier family." One customer had no qualms about pilfering cigarette butts from a man she suspected was her biological father, packaging them up, and shipping them off to GeneTree for paternity testing. "I was very excited to see that GeneTree had testing that could be done on cigarette butts," she admitted. She praised the confidentiality of the procedure, noting that no one involved—including the suspected father—"knows that I did the DNA test. I have both peace of mind and privacy."

I asked Terry Carmichael whether he considered it ethical to perform sensitive DNA testing without a person's knowledge or consent. "We ask for consent on all items that are tested, so whoever is submitting those items is providing the consent for testing them," he hedged. But what about the man whose cigarette butts GeneTree tested without his knowledge? "Look," he said, "my personal opinion, being an American, is that everyone should have the right to test whatever they have in their possession. If that's cigarette butts or a coffee mug or chewed gum, then they should be able to test it." Such is the consistent theme of GeneTree's marketing material: "Knowing the truth is always better than living in doubt," their website states with assurance. "DNA testing can help expose deceptions. DNA testing can expose lies and clear consciences."

GeneTree's website emphasizes the company's concern for privacy by offering reassuring platitudes ("your complete privacy guaranteed"), but it provides no information on the ultimate fate of the samples one submits for testing. The "Consent to DNA Testing Services Agreement" on the back of my free GeneTree paternity kit is equally vague: "By submitting specimens to GeneTree I agree to relinquish GeneTree and its representatives from all responsibility for the specimen collection and from any effects or actions that the results from this test may have on any individual."

When asked whether GeneTree would consider selling DNA profiles—or even the original samples themselves—to pharmaceutical companies or insurers, Carmichael conceded: "There is an interest in that," but "our policy is just to test the samples for what the customer wants us to test it for." He assured me that GeneTree is not yet in the business of selling its DNA samples, but other companies are headed in that direction. The most aggressive of these companies is Orchid Biosciences, which bills itself as "the leading provider of services and products for profiling genetic uniqueness." By buying up smaller genetic testing companies such as GeneScreen, CellMark, and Labcorp, Orchid has cornered about 35-45 percent of the market share in forensic and paternity DNA testing. Orchid's focus is on drug development for pharmaceutical companies, and some industry watchers speculate that Orchid's business plan is a harbinger of the industry's future—in which giant companies assemble large genetic databases, originally created for one purpose, which they use for drastically different ends.

Genetic Fingerprints and Human Liberty

The creation of new DNA databases and the expansion of existing ones show no signs of slowing. The National Commission on the Future of DNA Evidence (at the National Institute of Justice) projects that by 2005, the CODIS database will contain the DNA profiles of more than one million felons; by 2010 the commission "expects portable, miniaturized instrumentation that will provide analysis at the crime scene with computer-linked remote analysis." Paralleling these developments in forensic technology will be the increasing knowledge gained by geneticists about DNA markers. "In the future," the Commission concluded, "it is likely that an increasing number of suspects will be identified by database searches."

The resemblance of these new initiatives to crime-fighting schemes of earlier this century is telling. Criminals are often targeted first for the testing of novel social theories. Italian criminologist Cesare Lombroso's theories of hereditary criminal degeneracy prompted compulsory sterilization laws for criminals in several U.S. states in the early twentieth century. Eventually, as eugenic ideas took root in American soil, these compulsory sterilization laws—always billed as progressive measures to protect the public good—expanded to include ever-broader segments of the population. Researchers are already greedily eyeing the military's DNA database and CODIS as possible resources for locating genetic markers for certain behaviors, including criminal behavior. And it is not difficult to imagine the evolution of a system of criminal profiling based on genetic markers for traits such as aggression, which could then be introduced in criminal prosecutions. In Britain, for example, a recent report by the Nuffield Council on Bioethics suggested that the genetic causes of criminal behavior might eventually be considered as mitigating factors during sentencing of offenders.

As long as genetic samples are voluntary, anonymous, and privacy-protected, the benefits of DNA databases for fighting crime and improving medicine seem to outweigh the risks. At present, however, there is insufficient regulation and oversight of how private companies may use genetic information. Many businesses elide the standards of informed consent with statements that are deliberately misleading, and informed consent is itself an insufficient principle to guide our use of the new genetic technology. Indeed, many of the possible misuses of genetic information are not yet manifest, which makes true consent impossible.

Some of the challenges we face are clearly practical: ensuring the privacy or destruction of original samples; protecting databases from Internet hackers and computer criminals; ensuring access to one's own genetic information or genetic profile if others already possess it. Beyond merely practical concerns, however, it is worth considering what the mining and use of genetic information might mean for how we view ourselves and live our lives. Since the dawn of human reason, we have been intent on classifying the world around us. But the nature and scale of the classification we are now embarking on is altogether different from any we have done before. We live in a world that no longer tolerates the existence of a tomb of the unknowns. We complain that our local bank no longer sends us our cancelled checks, and yet we unthinkingly send our DNA out to be banked in perpetuity by strangers.

Ten years ago, Dorothy Nelkin, a professor at New York University, imagined "a kind of Jonathan Swift scenario—families demanding information about their genetic roots, adoption brokers probing the genetic history of children in order to find appropriate matches, or commercial firms storing genetic profiles and selling them to interested agencies." With the exception of adoption brokers, her predictions have come to pass. Today, information is power, but some information is not unambiguously good for us or others to possess. Not every person will want to know if they carry the gene for a debilitating condition. Not every parent will wish to test their offspring for genetic markers for height, aggression, or sexual orientation. As one writer recently confessed, after being approached by a distant relative to take a DNA test to establish their genealogical link, "It's just that the idea of part of my personal genetic code sitting in some database gives me the creeps."

In the 1997 movie "Gattaca," the main character, a member of the genetic underclass, spends tortured hours figuring out how to outwit the ubiquitous genetic sensors, linked to a universal DNA database, that instantly separate the genetically fit from the unfit. In this brave new society, the genetically weak (or "invalids") are not allowed to pursue certain jobs or romantic interests. Parents turn human procreation over to genetic designers. The society is high-achieving and super-efficient but despotic and stale.

Perhaps such a world seems absurd to us now; our guiding principle is liberty, we tell ourselves, which means allowing individuals to decide for them-

selves what to do with their genetic information. And yet, step-by-step and often for defensible reasons, we are paving the way for the universal, compulsory, DNA sampling of citizens. These are not simply the musings of science fiction; they are the logical conclusion of the technological infrastructure of DNA identification—such as Britain's Biobank—that we are eagerly building. In the beginning, the reasons for such databases will be familiar, modern, liberal, and compelling: to cure disease, to catch criminals, to ensure that children have a healthy beginning to their lives. But the end in sight is a drastically different society and way of life. We may come to know too much about ourselves to truly live in freedom; and our public and private institutions may know so much about us that equal treatment and personal liberty may become impossible.

We cannot escape our genes—not yet, at least. And we will probably never fully understand the relationship between our biology and our destiny. Human beings will always be at least partially a mystery, and therefore at least partially free. But we can escape or at least limit having our genetic profile spread promiscuously across unregulated, unprotected DNA databases. Participants in the DNA revolution—from forensic DNA database managers to Internet purveyors of paternity tests—are together poised to become one of the most powerful forces for determining the value of our DNA. Before going further down this path, we should pause to consider the benefits and dangers of allowing them to do so.